[0080] **CLAIMS**

What is claimed is:

1. A method comprising:

translating a credential with a corresponding one of a plurality of different credential provider modules each translating a corresponding different type of said credential into a common credential protocol;

communicating the translated credential having the common credential protocol through a credential provider Application Program Interface (API) to a logon user interface (UI) module of a native operating system (OS) of a local machine;

calling a logon routine for the OS to authenticate the translated credential against a credential database; and

logging on a user identified by the translated credential to access the local machine when the authentication is successful.

2. The method as defined in Claim 1, wherein the user is not logged on to the local machine until a plurality of said credentials have been translated by a respective said different credential provider module, communicated, and authenticated successfully.

3. The method as defined in Claim 1, wherein the user is not logged on to the local machine when the credentials are translated.

4. The method as defined in Claim 1, wherein the translating of the credential further comprises:

the logon UI module requesting a flat list of the credential provider modules;

the flat list being displayed on a display rendered by the logon UI module; and

a selection of the one said credential provider module from the flat list on the display.

5. The method as defined in Claim 1, wherein the calling of the logon routine for the OS to authenticate the translated credential against a credential database further comprises:

communicating the translated credential to a local Security Authority (LSA); and

determining the authentication with the LSA against the credential database that is selected from the group consisting of:

a local Security Accounts Manager (SAM) database;

a local database other than the SAM database;

a remote credential database;

a token protocol credential service;

a challenge and response protocol service; and

an Active Directory (AD) and Kerberos Distribution Center (KDC) at a domain remote from the local machine.

6. The method as defined in Claim 1, wherein each said credential provider module is interoperable, through a credential provider API, to the OS.

7. The method as defined in Claim 1, wherein each different type of the credentials is selected from the group consisting of a username and password, a hardware

token credential, a digital certificate credential, a smart card credential, a challenge and response protocol credential, an eye retina, a human face, a gate or walk, a handwriting specimen, a voice, a scent, a fingerprint, and another biometric sample.

8. A computer-readable medium comprising instructions that, when executed by a computer, perform the method of Claim 1.

9. A method comprising:

receiving a credential from a user at an input device in communication with a local machine having an OS;

translating the credential with one of different coexisting credential provider modules for translating respectively different types of credentials into a common credential protocol; and

using a component of the OS to authenticate the translated credential having the common credential protocol against a credential database; and

logging the user on with the OS to access the local machine when the authentication is successful.

10. The method as defined in Claim 9, wherein the logging of the user on further comprises logging the user on to the local machine after a plurality of said credentials have been received, translated by a respective said different coexisting credential provider module, and authenticated successfully.

11. The method as defined in Claim 9, wherein the user is not logged on to the local machine at the time when the translated credentials are authenticated.

12. The method as defined in Claim 9, wherein the use of the component of the OS to authenticate the translated credential having the common credential protocol against the credential database further comprises:

communicating the translated credential to an LSA; and

determining the authentication with the LSA against the credential database that is selected from the group consisting of:

a SAM database;

a local database other than the SAM database;

a remote credential database;

a token protocol credential service;

a challenge and response protocol service; and

an AD and KDC at a domain remote from the local machine.

13. The method as defined in Claim 9, wherein each said credential provider module is interoperable, through a credential provider API, to the component of the OS.

14. A computer-readable medium comprising instructions that, when executed by a computer, perform the method of Claim 9.

15. A method comprising: /

requesting a credential with an application executing at a local machine, the local machine having an OS to which a user is logged on, the local machine being in communication with an input device;

using one of different coexisting credential provider modules to gather the credential at the input device from the user; and

giving the gathered credential to the application for authentication, wherein:

each said credential provider module can gather a respectively different type of credential;

each said credential provider module interfaces through a credential provider API with the OS;

the credential provider API receives credentials gathered by any said credential provider module; and

each said credential provider module can provide a respective said type of credential that it gathers to the credential provider API for authentication of a principal in order to log on with the OS to access the local machine.

16. A computer-readable medium comprising instructions that, when executed by a computer, perform the method of Claim 15.

17. A method comprising:

receiving a credential from a user at an input device in communication with a local machine having an OS;

translating the credential with a credential provider module that corresponds to the input device, wherein:

the credential provider module is one of a plurality of coexisting different said credential provider modules; and

each said credential provider module can perform a translation of a respectively different type of said credential received at a different said input device in communication with the local machine; and

each said translation of each said credential is in a common credential protocol;

communicating the translated credential having the common credential protocol through a credential provider interface to a logon UI routine of the OS;

passing the translated credential having the common credential protocol to a logon routine of the OS from the logon UI routine;

authenticating the translated credential against a credential database with the logon routine of the OS; and

logging the user on to access the local machine with the OS when the authentication is successful.

18. The method as defined in Claim 17, wherein the logging the user on to access the local machine with the OS further comprises deferring the logging on of the user to access the local machined until the receiving, the translating, the communicating, the passing, and the authenticating successfully have been repeated for each of a plurality of said credentials.

19. The method as defined in Claim 17, wherein the user is not logged on to access the local machine when the translated credentials are authenticated against the credential database with the logon routine of the OS.

20. The method as defined in Claim 17, wherein the authenticating of the translated credential against the credential database with the logon routine of the OS further comprises:

communicating the translated credential to an LSA from the logon routine of the OS; and

determining the authentication with the LSA against the credential database that is selected from the group consisting of:

a SAM database;

a local database other than the SAM database;

a remote credential database;

a token protocol credential service;

a challenge and response protocol service; and

an AD and KDC at a domain remote from the local machine.

21. A computer-readable medium comprising instructions that, when executed by a computer, perform the method of Claim 17.

22. A computer-readable medium comprising a credential provider module including instructions that, when executed by a local machine having an OS, receive and translate a credential into a credential protocol so as to be compatible for authentication by

an authentication component of the OS against a credential database for logging a user identified by the credential on with the OS to access the local machine when the authentication is successful, wherein:

the translated credential can be received via an interface to the authentication component of the OS;

the interface to the authentication component of the OS is compatible for receiving each of a plurality of said credentials from a corresponding plurality of different coexisting credential provider modules; and

each said different coexisting credential provider module can:

receive a respective different type of said credential from a respective input device; and

translate each said different type of said credential into the credential protocol so as to be compatible for authentication by the authentication component of the OS against the credential database.

23. The computer-readable medium as defined in Claim 22, wherein the authentication component of the OS comprises:

a logon UI module;

an OS logon module for receiving Remote Procedure Call (RPC) calls from the log UI module; and

an LSA for determining the authentication, and in communication with, the credential database that is selected from the group consisting of:

a SAM database;

a local database other than the SAM database;

a remote credential database;

a token protocol credential service;

a challenge and response protocol service; and

an AD and KDC at a domain remote from the local machine.

24. A native OS comprising an authentication module to:

authenticate a user with a credential received from one of plurality of different and coexisting credential provider modules each translating a corresponding different type of user-input into the credential in a common credential protocol; and

log on the user identified by the translated credential to access the local machine when the authentication is successful.

25. A computer-readable medium comprising a pre-logon access provider (PLAP) module including instructions that, when executed by a local machine having an OS, receive a credential and an access service corresponding to the PLAP module;

establish a communication with a domain using the access service for authentication by an authentication component of the OS against a credential database for logging a user identified by the credential on with the OS to access the local machine when the authentication is successful, wherein:

the credential can be received via an interface to the authentication component of the OS;

the interface to the authentication component of the OS is compatible for receiving each of a plurality of said credentials and said access services from a corresponding plurality of different and coexisting said PLAP modules; and each said different coexisting PLAP module can establish a connection of a respective different type so as to be compatible for communications in the authentication by the authentication component of the OS against the credential database.

26. The computer-readable medium as defined in Claim 25, wherein the authentication component of the OS comprises:

a logon UI module;

an OS logon module for receiving RPC calls from the log UI module; and

an LSA for determining the authentication, and in communication with, the credential database that is selected from the group consisting of:

a SAM database;

a local database other than the SAM database;

a remote credential database;

a token protocol credential service;

a challenge and response protocol service; and

an AD and KDC at a domain remote from the local machine.

27. A native OS comprising a PLAP Manager API to an authentication module, wherein:

each of a plurality of different and coexisting PLAP modules can establish a connection between the PLAP Manager API and an access service corresponding to the PLAP module;

each said PLAP module specifies a credential and a corresponding different type of connection to the corresponding access service;

the authentication module authenticates a principal using the credential specified by one said PLAP module to access a local machine through the native OS; and

when the authentication of the principal is successful, the principal can use the local machine to communicate between the PLAP Manager API and the access service corresponding to the one said PLAP module.

28. A method comprising:

requesting, with a logon UI module of an OS through a PLAP manager API thereto, a flat list of access services from a corresponding plurality of coexisting and different PLAP modules;

displaying the flat list of access services on a display rendered by the logon UI module;

receiving an input of a credential and a selection of one said access service from the flat list of access services on the display;

when a connection to a domain is established using the one said access service:

passing the credential to an authentication provider at the domain;

performing a first authentication of the credential against the authentication provider at the domain; and

when the first authentication is successful:

communicating the credential from the PLAP API to the logon UI module;

performing an RPC call from the logon UI module passing the credential to an OS logon module;

passing the credential from the OS logon module with an LSA logon user call to an LSA;

performing a second authentication with the LSA against a credential database that is selected from the group consisting of:

a SAM database;

a local database other than the SAM database;

a remote credential database;

a token protocol credential service;

a challenge and response protocol service; and

an AD and KDC at a domain remote from the local machine;

when the second authentication is successful, logging on a user identified by the credential to use a local machine executing the OS.

29. The method as defined in Claim 28, further comprising, when the connection to the domain is not established using the one said access service:

redisplaying the flat list of access services on the display rendered by the logon UI module;

prompting for other credentials and another selection of one said access service;

receiving an input of the other credentials and the another selection of one said access service; and

attempting to establish a connection to a domain is using the another selection of one said access service.

30. In a computing device having a processor for executing an OS including an authentication component having a logon UI module, an OS logon module for receiving RPC calls from the logon UI module, an LSA for receiving LSA logon User calls from the OS logon module, wherein the LSA is in communication with one or more credential databases, wherein the computing device executes instructions in a computer-readable medium, and wherein the instructions comprise a plurality of different, coexisting, and respective PLAP and credential provider modules, wherein:

each said module communicates with an API to the logon UI module;

the logon UI module is compatible for receiving:

a credential; and

a selection of an access service specified by a corresponding said PLAP module;

the API can establish and maintain a network session via a connection to a domain using the selected access service when the received credential is authenticated by the API against the one or more credential databases at the domain;

the credential received by the logon UI module is translated with a corresponding one of the credential provider modules each translating a corresponding different type of said credential into a common credential protocol;

each said credential provider module communicates the translated credential having the common credential protocol through the API to the authentication component of the OS to authenticate the translated credential against the one or more credential databases; and

the authentication component of the OS logs on a user identified by the translated credential to access the local machine when the authentication is successful.

31. The computer-readable medium as defined in Claim 30, wherein the logon UI module comprised further instructions for:

requesting a flat list of:

a representation of credential providers from, and corresponding to, the credential provider modules; and

the access services from, corresponding to, the PLAP modules;

rendering a display of each said flat list; and

receiving one or more selection from each said flat list on the display.

32. The computer-readable medium as defined in Claim 30, wherein each different type of the credentials is selected from the group consisting of a username and password, a hardware token credential, a digital certificate credential, a smart card credential, a challenge and response protocol credential, an eye retina, a human face, a gate or walk, a handwriting specimen, a voice, a scent, a fingerprint, and another biometric sample.